



Department of Defense

DIRECTIVE

NUMBER 8500.01E

October 24, 2002

Certified Current as of April 23, 2007

ASD(NII)/DoD CIO

SUBJECT: Information Assurance (IA)

- References: (a) Section 2224 of title 10, United States Code, "Defense Information Assurance Program"
- (b) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988 (hereby canceled)
 - (c) DoD 5200.28-M, "ADP Security Manual," January 1973 (hereby canceled)
 - (d) DoD 5200.28-STD, "DoD Trusted Computer Security Evaluation Criteria," December 1985 (hereby canceled)
 - (e) through (ah), see enclosure 1

1. PURPOSE

This Directive:

1.1. Establishes policy and assigns responsibilities under reference (a) to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.

1.2. Supersedes DoD Directive 5200.28, DoD 5200.28-M, DoD 5200.28-STD, and DoD Chief Information Officer (CIO) Memorandum 6-8510 (references (b), (c), (d), and (e)).

1.3. Designates the Secretary of the Army as the Executive Agent for the integration of common biometric technologies throughout the Department of Defense.

1.4. Authorizes the publication of DoD 8500.1-M consistent with DoD 5025.1-M (reference (f)).

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 24 OCT 2002		2. REPORT TYPE		3. DATES COVERED 00-00-2002 to 00-00-2002	
4. TITLE AND SUBTITLE Information Assurance (IA)				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Department of Defense ,1400 Defense Pentagon,Washington,DC,20301-1400				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 22	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to:

2.1.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.1.2. All DoD-owned or -controlled information systems that receive, process, store, display or transmit DoD information, regardless of mission assurance category, classification or sensitivity, including but not limited to:

2.1.2.1. DoD information systems that support special environments, e.g., Special Access Programs (SAP) and Special Access Requirements (SAR), as supplemented by the special needs of the program.

2.1.2.2. Platform IT interconnections, e.g., weapons systems, sensors, medical technologies or utility distribution systems, to external networks.

2.1.2.3. Information systems under contract to the Department of Defense.

2.1.2.4. Outsourced information-based processes such as those supporting e-Business or e-Commerce processes.

2.1.2.5. Information systems of Nonappropriated Fund Instrumentalities.

2.1.2.6. Stand-alone information systems.

2.1.2.7. Mobile computing devices such as laptops, handhelds, and personal digital assistants operating in either wired or wireless mode, and other information technologies as may be developed.

2.2. Nothing in this policy shall alter or supercede the existing authorities and policies of the Director of Central Intelligence (DCI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 (reference (g)) and other laws and regulations.

2.3. This policy does not apply to weapons systems as defined by DoD Directive 5144.1 (reference (h)) or other IT components, both hardware and software, that are physically part of, dedicated to, or essential in real time to a platform's mission performance where there is no platform IT interconnection.

3. DEFINITIONS

Terms used in this Directive are defined in National Security Telecommunications and Information Systems Security Instruction Number 4009 (reference (i)) or enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems in accordance with 10 U.S.C. Section 2224, Office of Management and Budget Circular A-130, Appendix III, DoD Directive 5000.1 (references (a), (j), and (k)), this Directive, and other IA-related DoD guidance, as issued.

4.2. All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system; and cost effectiveness. For IA purposes all DoD information systems shall be organized and managed in the four categories defined in enclosure 2: automated information system (AIS) applications, enclaves (which include networks), outsourced IT-based processes, and platform IT interconnections.

4.3. Information assurance shall be a visible element of all investment portfolios incorporating DoD-owned or -controlled information systems, to include outsourced business processes supported by private sector information systems and outsourced information technologies; and shall be reviewed and managed relative to contributions to mission outcomes and strategic goals and objectives, in accordance with 40 U.S.C. Sections 1423 and 1451 (reference (l)). Data shall be collected to support reporting and IA management activities across the investment life cycle.

4.4. Interoperability and integration of IA solutions within or supporting the Department of Defense shall be achieved through adherence to an architecture that will enable the evolution to network centric warfare by remaining consistent with the Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance Architecture Framework, and a defense-in-depth approach. This combination produces layers of technical and non-technical solutions that: provide appropriate levels of confidentiality, integrity, authentication, non-repudiation, and availability; defend the perimeters of enclaves; provide appropriate degrees of protection to all enclaves and computing environments; and make appropriate use of supporting IA infrastructures, to include robust key management and incident detection and response.

4.5. The Department of Defense shall organize, plan, assess, train for, and conduct the defense of DoD computer networks as integrated computer network defense (CND) operations that are coordinated across multiple disciplines in accordance with DoD Directive O-8530.1 (reference (m)).

4.6. Information assurance readiness shall be monitored, reported, and evaluated as a distinguishable element of mission readiness throughout all the DoD Components, and validated by the DoD CIO.

4.7. All DoD information systems shall be assigned a mission assurance category that is directly associated with the importance of the information they contain relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Requirements for availability and integrity are associated with the mission assurance category, while requirements for confidentiality are associated with the information classification or sensitivity and need-to-know. Both sets of requirements are primarily expressed in the form of IA controls and shall be satisfied by employing the tenets of defense-in-depth for layering IA solutions within a given IT asset and among assets; and ensuring appropriate robustness of the solution, as determined by the relative strength of the mechanism and the confidence that it is implemented and will perform as intended. The IA solutions that provide availability, integrity, and confidentiality also provide authentication and non-repudiation.

4.8. Access to all DoD information systems shall be based on a demonstrated need-to-know, and granted in accordance with applicable laws and DoD 5200.2-R (reference (n)) for background investigations, special access and IT position designations and requirements. An appropriate security clearance and non-disclosure agreement are also required for access to classified information in accordance with DoD 5200.1-R (reference (o)). Further:

4.8.1. The minimum requirement for DoD information system access shall be a properly administered and protected individual identifier and password.

4.8.2. The use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication shall be in accordance with published DoD policy and procedures. These technologies shall be incorporated in all new acquisitions and upgrades whenever possible. Where interoperable PKI is required for the exchange of unclassified information with vendors and contractors, the Department of Defense shall only accept PKI certificates obtained from a DoD-approved external certificate authority or other mechanisms approved in accordance with DoD policy.

4.9. In addition to the requirements in paragraph 4.8., foreign exchange personnel and representatives of foreign nations, coalitions or international organizations may be authorized access to DoD information systems containing classified or sensitive information only if all of the following conditions are met:

4.9.1. Access is authorized only by the DoD Component Head in accordance with the Department of Defense, the Department of State (DoS), and DCI disclosure and interconnection policies, as applicable.

4.9.2. Mechanisms are in place to strictly limit access to information that has been cleared for release to the represented foreign nation, coalition or international organization, (e.g., North Atlantic Treaty Organization) in accordance with DoD Directive 5230.11 (reference (p)), for classified information, and other policy guidance for unclassified information such as reference (o), DoD Directive 5230.20E (reference (q)), and DoD Instruction 5230.27 (reference (r)).

4.10. Authorized users who are contractors, DoD direct or indirect hire foreign national employees, or foreign representatives as described in paragraph 4.9., above, shall always have their affiliation displayed as part of their e-mail addresses.

4.11. Access to DoD-owned, -operated or -outsourced web sites shall be strictly controlled by the web site owner using technical, operational, and procedural measures appropriate to the web site audience and information classification or sensitivity.

4.11.1. Access to DoD-owned, -operated or -controlled web sites containing official information shall be granted according to reference (o) and need-to-know rules established by the information owner.

4.11.2. Access to DoD-owned, -operated or -controlled web sites containing public information is not restricted; however, the information accessible through the web sites shall be limited to unclassified information that has been reviewed and approved for release in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29 (references (s) and (t)).

4.12. DoD information systems shall regulate remote access and access to the Internet by employing positive technical controls such as proxy services and screened subnets, also called demilitarized zones (DMZ), or through systems that are isolated from all other DoD information systems through physical means. This includes remote access for telework.

4.13. All DoD information systems shall be certified and accredited in accordance with DoD Instruction 5200.40 (reference (u)).

4.14. All interconnections of DoD information systems shall be managed to continuously minimize community risk by ensuring that the assurance of one system is not undermined by vulnerabilities of interconnected systems.

4.14.1. Interconnections of Intelligence Community (IC) systems and DoD information systems shall be accomplished using a process jointly established by the DoD CIO and the IC CIO.

4.14.2. Connection to the Defense Information System Network (DISN) shall comply with connection approval procedures and processes, as established.

4.14.3. Interconnections among DoD information systems of different security domains or with other U.S. Government systems of different security domains shall be employed only to meet compelling operational requirements, not operational convenience. Secure configurations of approved IA and IA-enabled IT products, uniform risk criteria, trained systems security personnel, and strict configuration control shall be employed. The community risk shall be assessed and measures taken to mitigate that risk in accordance with procedures established by the DISN Designated Approving Authorities (DAAs) prior to interconnecting the systems.

4.14.4. The interconnection of DoD information systems with those of U.S. allies, foreign nations, coalition partners, or international organizations shall comply with applicable international agreements and, whenever possible, DoD IA policies. Variations shall be approved by the responsible Combatant Commander and the DISN DAAs, and incorporated in the system security documentation. Information provided through these interconnections must be released in accordance with reference (o) or reference (p).

4.15. All DoD information systems shall comply with DoD ports and protocols guidance and management processes, as established.

4.16. The conduct of all DoD communications security activities, including the acquisition of COMSEC products, shall be in accordance with DoD Directive C-5200.5 (reference (v)).

4.17. All IA or IA-enabled IT hardware, firmware, and software components or products incorporated into DoD information systems must comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 (reference (w)). Such products must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase; i.e., vendors will warrant, in their responses to a solicitation and as a condition of the contract, that the vendor's products will be satisfactorily validated within a period of time specified in the solicitation and the contract. Purchase contracts shall specify that product validation will be maintained for updated versions or modifications by subsequent evaluation or through participation in the National IA Partnership (NIAP) Assurance Maintenance Program.

4.18. All IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines.¹

4.19. Public domain software products, and other software products with limited or no warranty, such as those commonly known as freeware or shareware, shall only be used in DoD information systems to meet compelling operational requirements. Such products shall be thoroughly assessed for risk and accepted for use by the responsible DAA.

¹ Guidelines are available at <http://iase.disa.mil/> and <http://www.nsa.gov/>

4.20. DoD information systems shall be monitored based on the assigned mission assurance category and assessed risk in order to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the IA of DoD operations or IT resources, including internal misuse. DoD information systems also shall be subject to active penetrations and other forms of testing used to complement monitoring activities in accordance with DoD and Component policy and restrictions.

4.21. Identified DoD information system vulnerabilities shall be evaluated for DoD impact, and tracked and mitigated in accordance with DoD-directed solutions, e.g., Information Assurance Vulnerability Alerts.

4.22. All personnel authorized access to DoD information systems shall be adequately trained in accordance with DoD and Component policies and requirements and certified as required in order to perform the tasks associated with their IA responsibilities.

4.23. Individuals shall be notified of their privacy rights and security responsibilities in accordance with DoD Component General Counsel-approved processes when attempting access to DoD information systems.

4.24. Mobile code technologies shall be categorized and controlled to reduce their threat to DoD information systems in accordance with DoD and Component policy and guidance.

4.25. A DAA shall be appointed for each DoD information system operating within or on behalf of the Department of Defense, to include outsourced business processes supported by private sector information systems and outsourced information technologies. The DAA shall be a U.S. citizen, a DoD employee, and have a level of authority commensurate with accepting, in writing, the risk of operating DoD information systems under his or her purview.

4.26. All military voice radio systems, to include cellular and commercial services, shall be protected consistent with the classification or sensitivity of the information transmitted on the system.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for *Networks and Information Integration*, as the DoD Chief Information Officer, shall:

5.1.1. Monitor, evaluate and provide advice to the Secretary of Defense regarding all DoD IA activities.

5.1.2. Oversee appropriations earmarked for the DoD IA program and manage the supporting activities of the office of the Defense-wide Information Assurance Program (DIAP) Office in accordance with reference (a).

5.1.3. Develop and promulgate additional IA policy guidance consistent with this Directive to address such topics as ports and protocols management, vulnerability management, biometrics, security management, IA education and training, mobile code, and interconnection between security domains.

5.1.4. Ensure the integration of IA initiatives with critical infrastructure protection sector liaisons, as defined in DoD Directive 3020.40 (reference (x)).

5.1.5. Establish a formal coordination process with the IC CIO to ensure proper protection of IC information within the Department of Defense.

5.1.6. Establish metrics and annually validate the IA readiness of all DoD Components as an element of mission readiness.

5.1.7. Ensure that responsibilities for IA aspects of Major Defense Acquisition Program design are integrated into existing Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) and Service Acquisition Executive processes.

5.1.8. Require the Director, Defense Information Systems Agency (DISA) to:

5.1.8.1. Develop, implement and oversee a single IA approach for layered protection (defense-in-depth) of the DISN in coordination with the Chairman of the Joint Chiefs of Staff, Director, Defense Intelligence Agency (DIA) and Director, National Security Agency (NSA).

5.1.8.2. Establish and manage connection approval processes for the DISN.

5.1.8.3. Develop and provide IA training and awareness products.

5.1.8.4. Develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.

5.1.8.5. Establish and implement:

5.1.8.5.1. A DoD ports and protocols management process.

5.1.8.5.2. Procedures for mitigation of risks associated with the use of mobile code in DoD information systems.

5.1.8.5.3. A web-based resource providing access to current DoD and Federal IA and IA-related policy and guidance, including recent and pending legislation.

5.1.9. Require the Director, Defense Intelligence Agency to:

5.1.9.1. Provide finished intelligence on IA, including threat assessments, to the DoD Components.

5.1.9.2. Develop, implement, and oversee an IA program for layered protection of the DoD non-cryptologic SCI systems including the DoD Intelligence Information System (DoDIIS) on the basis of defined DoD information systems and geographical or organizational boundaries.

5.1.9.3. Certify and accredit DoD non-cryptologic SCI and DoDIIS applications, enclaves, platform IT interconnections, and outsourced IT-based processes, and develop and provide an IA education, training, and awareness program for DoD non-cryptologic SCI systems and DoDIIS users and administrators.

5.1.9.4. Establish and manage a connection-approval process for the Joint Worldwide Intelligence Communications System.

5.1.10. Require the Director, Defense Security Service to monitor information system security practices and conduct regular inspections of DoD contractors processing classified information in accordance with DoD 5220.22-M (reference (y)).

5.2. The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) shall:

5.2.1. Require the Director, Defense Research and Engineering (DDR&E) to:

5.2.1.1. Monitor and oversee, in coordination with the Defense-wide Information Assurance Program Office, all Defense-wide IA research and technology investments and activities to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques.

5.2.1.2. Require the Director, Defense Advanced Research Projects Agency (DARPA) to coordinate all DoD IA research and technology initiatives under DARPA's purview with the Director, NSA.

5.2.2. Integrate policies established by this Directive and reference (w) into acquisition policy and guidance to include the Federal Acquisition Regulations System (reference (z)), and incorporate such policies into acquisitions under his or her purview.

5.2.3. Oversee IA assessments, in coordination with the Director, Operational Testing and Evaluation.

5.3. The Under Secretary of Defense for Personnel and Readiness shall, in coordination with the ASD(*NI*), develop and implement IA personnel management and skill tracking procedures and processes to ensure adequate personnel resources are available to meet critical DoD IA requirements.

5.4. The OSD Principal Staff Assistants shall:

5.4.1. Ensure end-to-end protection of information flows in their functional areas by guiding investments and other actions relating to IA.

5.4.2. Ensure that IA requirements for DoD information systems developed under their cognizance are fully coordinated at the DoD Component level and with the DIAP.

5.4.3. Appoint DAAs for Joint and Defense-wide information systems under their purview (e.g., the Defense Civilian Personnel Data System, Defense Message System, Defense Travel System, and the Joint Total Asset Visibility System).

5.4.4. Identify and include IA requirements in the design, acquisition, installation, operation, upgrade or replacement of all DoD information systems under their purview.

5.5. The Secretary of the Army shall serve as the Executive Agent for the integration of common biometric technologies throughout the Department of Defense.

5.6. The Chairman of the Joint Chiefs of Staff shall:

5.6.1. Serve as the principal military advisor to the Secretary of Defense on IA.

5.6.2. Ensure, in coordination with the ASD(*NI*), the validation of IA requirements for systems supporting Joint and Combined operations through the Joint Requirements Oversight Council.

5.6.3. Develop, coordinate, and promulgate IA policies, doctrine and procedures for Joint and Combined operations.

5.7. The Commander, United States Strategic Command, shall coordinate and direct DoD-wide CND operations in accordance with reference (m).

5.8. The Director, National Security Agency (NSA), shall:

5.8.1. Implement an IA intelligence capability responsive to requirements for the Department of Defense, less DIA responsibilities.

5.8.2. Provide IA support to the DoD Components as required in order to assess the threats to, and vulnerabilities of, information technologies.

5.8.3. Serve as the DoD focal point for IA cryptographic research and development in accordance with DDR&E direction and in coordination with the Director, DARPA.

5.8.4. Manage the development of the IA Technical Framework (reference (a)) in support of defense-in-depth, and provide engineering support and other technical assistance for its implementation within the Department of Defense.

5.8.5. Serve as the DoD focal point for the NIAP and establish criteria and processes for evaluating and validating all IA and IA-enabled IT products used in DoD information systems.

5.8.6. Plan, design, and manage the implementation of the Key Management Infrastructure/PKI within the Department of Defense.

5.8.7. In coordination with the USD(AT&L), develop and maintain an information system security engineering process that supports IT acquisition.

5.8.8. Support the Director, Defense Information Systems Agency in the development of security configuration guidance for IA and IA-enabled IT products.

5.8.9. Develop, implement, and oversee an IA program for layered protection of DoD cryptologic SCI systems, an IA certification and accreditation process for DoD cryptologic SCI applications, enclaves, platform IT interconnections and outsourced IT-based processes, and an IA education, training, and awareness program for users and administrators of DoD cryptologic SCI systems.

5.9. The Director, Operational Testing and Evaluation, shall oversee IA assessments.

5.10. The Heads of the DoD Components shall:

5.10.1. Develop and implement an IA program focused on assurance of DoD Component-specific information and systems (e.g., sustaining base, tactical, and Command, Control, Communications, Computers, and Intelligence (C4I) interfaces to weapon systems) that is consistent with references (a) and (l) and defense-in-depth.

5.10.2. Coordinate with Joint and Defense-wide program offices to ensure interoperability of IA solutions across the DoD enterprise.

5.10.3. Collect and report IA management, financial, and readiness data to meet DoD IA internal and external reporting requirements.

5.10.4. Appoint DAAs for all DoD information systems for which they have responsibility.

5.10.5. Identify and include IA requirements in the design, acquisition, installation, operation, upgrade or replacement of all DoD information systems for which they have responsibility.

5.10.6. Ensure that the Government's contract requirements properly reflect that IA or IA-enabled IT products are involved and must be properly evaluated and validated in accordance with paragraph 4.17., above.


5.10.7. Ensure that IA awareness, training, education, and professionalization are provided to all Component personnel commensurate with their respective responsibilities for developing, using, operating, administering, maintaining, and retiring DoD information systems.

5.10.8. Comply with established accreditation and connection approval processes required for all DoD information systems.

5.10.9. Coordinate all IA research and technology initiatives under their purview with the DDR&E.

6. EFFECTIVE DATE

This Directive is effective immediately.



Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 2

E1. References, continued

E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD CIO Memorandum 6-8510, "Guidance and Policy for Department of Defense Global Information Grid Information Assurance," June 16, 2000 (hereby canceled)
- (f) DoD 5025.1-M, "DoD Directives System Procedures," *March 5, 2003*
- (g) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- (h) DoD Directive *5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005*
- (i) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, "National Information Systems Security Glossary," September 2000²
- (j) OMB Circular A-130, "Management of Federal Information Resources, Transmittal 4," November 30, 2000
- (k) DoD Directive 5000.1, "The Defense Acquisition System," *May 12, 2003*
- (l) Sections 1423 and 1451 of title 40, United States Code, "Division E of the Clinger-Cohen Act of 1996"
- (m) DoD Directive O-8530.1, "Computer Network Defense," January 8, 2001
- (n) DoD 5200.2-R, "DoD Personnel Security Program," *December 16, 1986*
- (o) DoD 5200.1-R, "DoD Information Security Program Regulation," January 14, 1997
- (p) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
- (q) DoD Directive 5230.20E, "Visits *and* Assignments of Foreign Nationals," *June 22, 2005*
- (r) DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," October 6, 1987
- (s) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996
- (t) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 6, 1999
- (u) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP)," December 30, 1997
- (v) DoD Directive C-5200.5, "Communications Security (COMSEC)," (U) April 21, 1990
- (w) National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-enabled Information Technology Products," January 2000
- (x) DoD Directive *3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005*
- (y) DoD 5220.22-M, "National Industrial Security Program Operating Manual," January 1995 and "National Industrial Security Program Operating Manual Supplement," February 1995

² Available at <http://www.nstissc.gov/html/library.html>

- (z) Title 48, Code of Federal Regulations, "Federal Acquisition Regulations System," October 1, 1996³
- (a*a*) Information Assurance Technical Framework (IATF), Release 3.0, September 2000⁴
- (a*b*) DoD 7000.14-R, Vol 2B, Chapter 5, "DoD Financial Management Regulation," June 2000
- (a*c*) Section 552a of title 5, United States Code, "The Privacy Act of 1974"
- (a*d*) Section 278g-3 of title 15, United States Code, "Computer Security Act of 1987"
- (a*e*) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998
- (a*f*) Section 552 of title 5, United States Code, "Freedom of Information Act"
- (a*g*) DoD Directive 5210.83, "Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI)", November 15, 1991
- (a*h*) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984

³ Available at <http://web1.deskbook.osd.mil/htmlfiles/rlcats.asp>

⁴ Available at <http://www.iatf.net>

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Application. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs.

E2.1.2. Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (reference (i)).

E2.1.3. Authorized User. Any appropriately cleared individual with a requirement to access a DoD information system in order to perform or assist in a lawful and authorized governmental function.

E2.1.4. Availability. Timely, reliable access to data and information services for authorized users (reference (i)).

E2.1.5. Community Risk. Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.

E2.1.6. Computer Network. The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities such as local or campus area networks, or long-haul data transport capabilities such as operational, metropolitan, or wide area and backbone networks.

E2.1.7. Computing Environment. Workstation or server (host) and its operating system, peripherals, and applications (reference (i)).

E2.1.8. Confidentiality. Assurance that information is not disclosed to unauthorized entities or processes (reference (i)).

E2.1.9. Connection Approval. Formal authorization to interconnect information systems.

E2.1.10. Controlled Unclassified Information. A term used, but not specifically defined in reference (o), to refer to sensitive information as defined in paragraph E2.1.41., below.

E2.1.11. Defense-in-Depth. The DoD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among IT assets; and, the selection of IA solutions based on their relative level of robustness.

E2.1.12. Defense Information System Network (DISN). The DoD consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations.

E2.1.13. Designated Approving Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority (reference (i)).

E2.1.14. DISN Designated Approving Authority (DISN DAA). One of four DAAs responsible for operating the DISN at an acceptable level of risk. The four DISN DAAs are the Directors of the DISA, the DIA, the NSA and the Director of the Joint Staff (delegated to the Joint Staff Director for Command, Control, Communications, and Computer Systems (J-6)).

E2.1.15. DMZ (Demilitarized Zone). Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's IA policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks. A DMZ is also called a "screened subnet."

E2.1.16. DoD Information System. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

E2.1.16.1. Automated Information System (AIS) Application. For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program, such as those described in reference (k). An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense

Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note that an AIS application is analogous to a "major application" as defined in reference (j); however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System.

E2.1.16.2. Enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in reference (j). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

E2.1.16.3. Outsourced IT-based Process. For DoD IA purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

E2.1.16.4. Platform IT Interconnection. For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.

E2.1.17. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.1.18. IA Certification and Accreditation. The standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems.

E2.1.19. IA Control. An objective IA condition of integrity, availability or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control class. Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with reference (j).

E2.1.20. IA Product. Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.

E2.1.21. IA-Enabled Information Technology Product. Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

E2.1.22. Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

E2.1.23. Integrity. Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (reference (i)).

E2.1.24. IT Position Category. Applicable to unclassified DoD information systems, a designator that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Position categories include: IT-I (Privileged), IT-II (Limited Privileged) and IT-III (Non-Privileged), as defined in reference (o). Investigative requirements for each category vary, depending on role and whether the incumbent is a U.S. military member, U.S. civilian government employee, U.S. civilian contractor or a foreign national. The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position.

E2.1.25. Mission Assurance Category (MAC). Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

E2.1.25.1. Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

E2.1.25.2. Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.

E2.1.25.3. Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

E2.1.26. Mobile Code. Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

E2.1.27. National Information Assurance Partnership (NIAP). Joint initiative between the NSA and the National Institute of Standards and Technology responsible for security testing needs of both IT consumers and producers and promoting the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems.

E2.1.28. Need-to-Know. Necessity for access to, or knowledge or possession of, specific official DoD information required to carry out official duties (reference (i) modified).

E2.1.29. Need-to-Know Determination. Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties (reference (i)).

E2.1.30. Non-repudiation. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data (reference (i)).

E2.1.31. Official DoD Information. All information that is in the custody and control of the Department of Defense, relates to information in the custody and control of the Department, or was acquired by DoD employees as part of their official duties or because of their official status within the Department (reference (s)).

E2.1.32. Portfolio. The aggregate of IT investments for DoD information systems, infrastructure and related technical activities that are linked to mission goals, strategies, and architectures, using various assessment and analysis tools to permit information and IT decisions to be based on their contribution to the effectiveness and efficiency of military missions and supporting business functions. Portfolios enable the Department of Defense to manage IT resources and align strategies and programs with Defense-wide, functional, and organizational goals and measures.

E2.1.33. Proxy. Software agent that performs a function or operation on behalf of another application or system while hiding the details involved. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client network address is authorized to use the requested service, optionally perform additional authentication, and then complete a connection on behalf of the user to a remote destination.

E2.1.34. Public Domain Software. Software not protected by copyright laws of any nation that carries no warranties or liabilities, and may be freely used without permission of or payment to the creator.

E2.1.35. Public Information. Official DoD information that has been reviewed and approved for public release by the information owner in accordance with reference (s).

E2.1.36. Research and Technology. Activities that may be described as basic research, applied research, and advanced technology development, demonstrations or equivalent activities, regardless of budget activity. Definitions for Basic Research, Applied Research and Advanced Technology Development are provided in the DoD FMR, Chapter 5 (reference (a**b**)).

E2.1.37. Robustness. A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. The Department of Defense has three levels of robustness:

E2.1.37.1. High Robustness: Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.

E2.1.37.2. Medium Robustness: Security services and mechanisms that provide for layering of additional safeguards above good commercial practices.

E2.1.37.3. Basic Robustness: Security services and mechanisms that equate to good commercial practices.

E2.1.38. Security Domain. Within an information system, the set of objects that is accessible. Access is determined by the controls associated with information properties such as its security classification, security compartment or sensitivity. The controls are applied both within the information system and in its connection to other classified or unclassified information systems.

E2.1.39. Sensitive But Unclassified (SBU). A term commonly and inappropriately used within the Department of Defense as a synonym for Sensitive Information, which is the preferred term.

E2.1.40. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

E2.1.41. Sensitive Information. Information the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, "The Privacy Act" (reference (ac)), but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of title 15, United States Code, "The Computer Security Act of 1987" (reference (ad)).) This includes information in routine DoD payroll, finance, logistics, and personnel management systems. Sensitive information sub-categories include, but are not limited to the following:

E2.1.41.1. For Official Use Only (FOUO). In accordance with DoD 5400.7-R (reference (ae)), DoD information exempted from mandatory public disclosure under the Freedom of Information Act (FOIA) (reference (af)).

E2.1.41.2. Privacy Data. Any record that is contained in a system of records, as defined in the reference (ac) and information the disclosure of which would constitute an unwarranted invasion of personal privacy.

E2.1.41.3. DoD Unclassified Controlled Nuclear Information (DoD UCNI). Unclassified information on security measures (security plans, procedures and equipment) for the physical protection of DoD Special Nuclear Material (SNM), equipment, or facilities in accordance with DoD Directive 5210.83 (reference (ag)). Information is Designated DoD UCNI when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities.

E2.1.41.4. Unclassified Technical Data. Data that is not classified, but is subject to export control and is withheld from public disclosure according to DoD Directive 5230.25 (reference (ah)).

E2.1.41.5. Proprietary. Information that is provided by a source or sources under the condition that it not be released to other sources.

E2.1.41.6. Foreign Government Information. Information that originated from a foreign government and that is not classified CONFIDENTIAL or higher, but must be protected in accordance with reference (o).

E2.1.41.7. Department of State Sensitive But Unclassified (DoS SBU). Information which originated from the DoS that has been determined to be SBU under appropriate DoS information security policies.

E2.1.41.8. Drug Enforcement Administration (DEA) Sensitive Information. Information originated by the DEA that requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.

E2.1.42. Supporting IA Infrastructures. Collections of interrelated processes, systems, and networks that provide a continual flow of information assurance services throughout the Department of Defense, e.g., the key management infrastructure or the incident detection and response infrastructure.

E2.1.43. Telework. Any arrangement in which an employee performs officially assigned duties at an alternative worksite on either a regular and recurring, or on an ad hoc, basis (not including while on official travel).